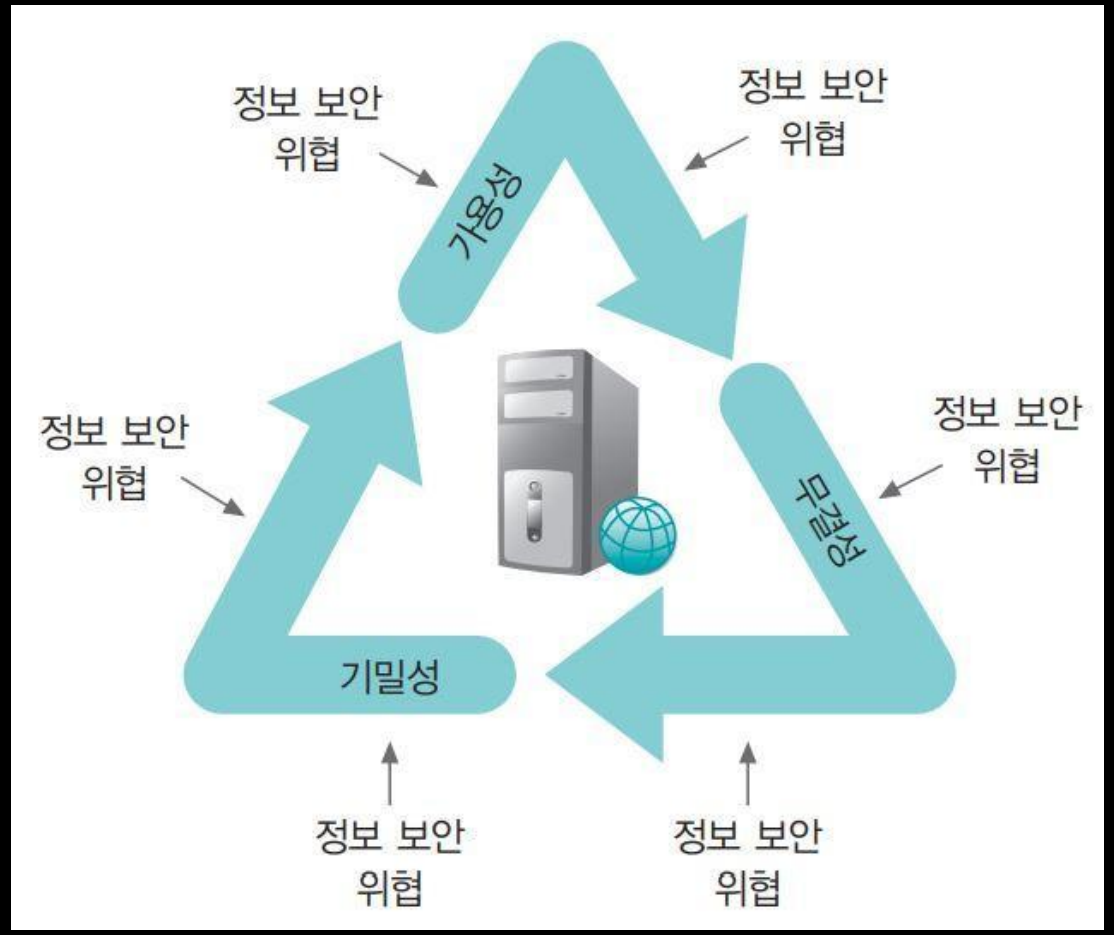
인공지능 보안
-03-
시스템 보안

보안의 3(+1)대 요소



+ 부인 방지

시스템 보안

시스템 보안 주제

- 계정 관리
  - 사용자를 식별하는 가장 기본적인 인증 수단은 아이디와 패스워드
- 세션 관리
  - 일정 시간이 지나면 세션을 종료하고 비인가자의 세션 가로채기를 통제
- 접근 제어
  - 네트워크 안에서 다른 시스템으로부터 적절히 보호할 수 있도록 접근을 통제
- 권한 관리
  - 각 사용자가 적절한 권한으로 적절하게 정보 자산에 접근하도록 통제
- 로그 관리
  - 시스템 내부나 네트워크를 통해 외부에서 시스템에 어떤 영향을 미칠 경우 그 내용을 기록하여 관리
- 취약점 관리
  - 시스템 자체의 결함을 체계적으로 관리

계정 관리

- 식별과 인증
  - 식별: 어떤 시스템에 로그인하려면 먼저 자신이 누군지를 알림
  - 인증: 로그인을 허용하기 위한 확인
- 보안의 네 가지 인증 방법
  - 알고 있는 것
    - 머릿속에 기억하고 있는 정보를 이용하여 인증 수행
  - 가지고 있는 것
    - 신분증이나 OTP 장치 등으로 인증 수행
  - 자신의 모습
    - 홍채와 같은 생체 정보로 인증 수행
  - 위치하는 곳
    - 현재 접속을 시도하는 위치의 적절성을 확인하거나 콜백을 사용해 인증 수행
    - 콜백: 접속을 요청한 사람의 신원을 확인, 미리 등록된 전화번호로 전화를 되걸어 접속을 요청한 사람이 본인인지 확인

세션 관리

- 세션
  - 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속
  - 예) 줄서고 있을 때 친구에게 자리 맡아달라고 부탁하기

- 지속적인 인증
  - 세션을 유지하기 위한 보안 사항
  - 인증에 성공한 후 인증된 사용자가 처음의 사용자인지 지속적으로 재인증
  - 매번 패스워드를 입력 할 수 없으므로 시스템은 이를 세션에 대한 타임아웃 설정으로 보완 (윈도우의 화면보호기)
  - 유닉스는 원격에서 접속할 경우 패스워드를 다시 묻지 않고 세션을 종료한 후 재접속할 것을 요구

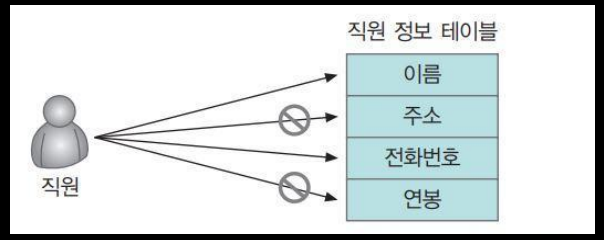
접근 제어

- 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근하도록 통제
- 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단
- 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트
- 운영체제에 대한 적절한 접근 제어를 수행하려면 가장 먼저 운영체제에서 어떤 인터페이스가 운영되고 있는지를 파악해야 함

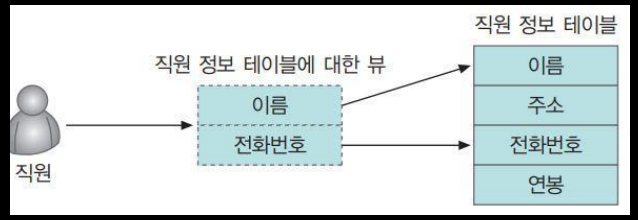
운영체제	서비스 이름	사용 포트	특징
유닉스 (리눅스 포함)	텔넷	23	암호화되지 않음
	SSH	22	SFTP 가능
	XDMCP	6000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴		VNC, Radmin 등

권한 관리

- 부여된 권한에 적합한 수준의 정보에 접근
- 데이터베이스의 권한 관리
  - 뷰에 대한 권한 관리
    - 뷰: 참조 테이블의 각 열에 대해 사용자의 권한을 설정하는 것이 불편해서 만든 가상 테이블
  - 뷰를 사용하지 않는 경우 테이블에 각각 접근 제한을 설정해야 함

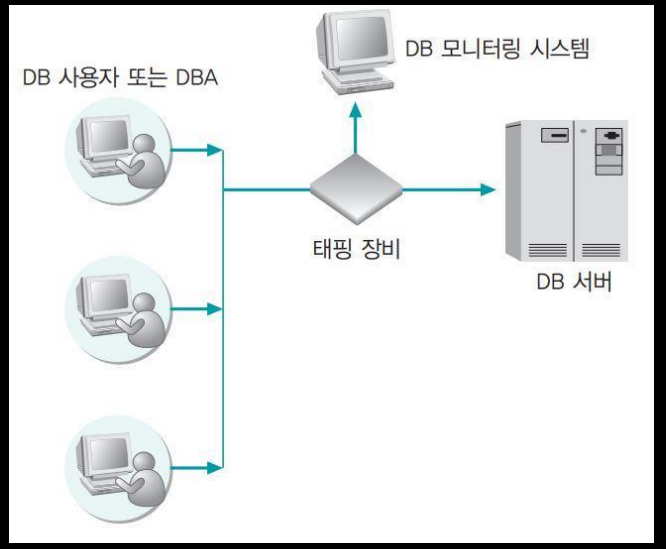


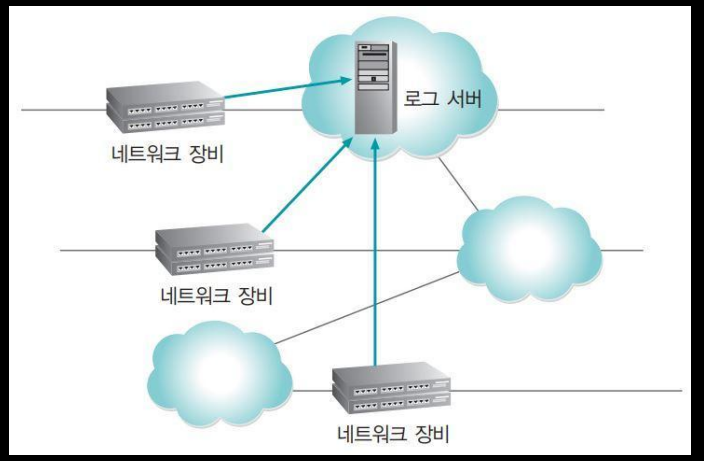
  - 뷰에 대한 권한만 할당



로그 관리

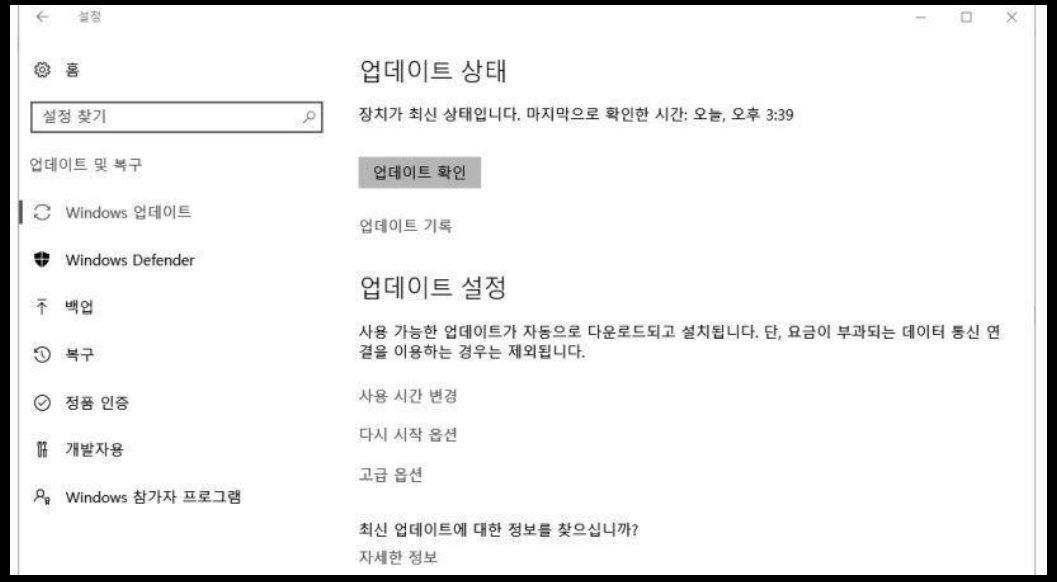
- 시스템 이용 내역을 기록
- 해커나 시스템에 접근한 악의적인 사용자를 추적
- 데이터베이스 모니터링
  - 네트워크 트래픽을 모니터링할 수 있는 태핑 장비를 네트워크에 설치
  - 네트워크 패킷 중에서 데이터베이스 질의문을 확인하여 이를 로그로 남김
  - 데이터베이스의 성능에 영향을 미치지 않으면서 잘못된 접근 시도와 질의문 입력을 모두 모니터링할 수 있음
- 네트워크 로깅
  - 대부분의 네트워크 장비에는 하드디스크와 같이 로그를 저장할 저장 공간이 없어 로그 서버를 별도로 두고 운영
  - 로그서버를 운용하면 해커가 어떤 네트워크 장비에 침투하더라도 자신의 흔적을 지우기가 쉽지 않음 (WORM 장비)
  - 이 때문에 네트워크 장비 뿐만 아니라 운영체제 등을 관리할 때 로그 서버를 따로 운영





취약점 관리

- 응용 프로그램을 만든 제작사가 배포하는 패치 또는 서비스 팩을 적용해 시스템 자체의 취약점을 보완
- 유닉스 시스템에도 내재된 취약점이 있지만 윈도우는 사용률이 훨씬 높고 접근하기도 쉬워 공격을 더 많이 받음
- 윈도우 업데이트를 통해 자동으로 보안 패치를 확인하고 적용할 수 있음
- 제로데이 공격(Zero-Day Attack)



Q&A